EPCglobal UHF Class-1 Generation-2 기반 RFID 시스템에 적합한 상호 인증 프로토콜 설계+

*원태연 **천지영 ***최은영 ****이동훈
고려대학교 정보경영공학전문 대학원
*kucs226@korea.ac.kr **jychun@korea.ac.kr ***bluecey@cist.korea.ac.kr
****donghlee@korea.ac.kr

Mutual Authentication Protocol suitable to RFID System based on EPCglobal UHF Class-1 Generation-2

*Won, Tae-Youn **Chun, Ji-Young ***Choi, Eun-Young ****Lee, Dong-Hoon
Graduate School of Information Management & Security

요약

일정한 라디오 주파수 대역을 이용해 무선 방식으로 사물을 식별하는 RFID 시스템의 보안 및 프라이버시 보호를 위한 많은 기법들이 제안되었다. 하지만 제안된 기법들의 대부분은 국제 표준인 Class-1 Generation-2 태그에는 적합하지 않으며 안전성에서도 취약성이 있다. 최근에 Chien과 Chen은 Class-1 Generation-2 태그에 적합하면서도 안전성이 보장되는 상호 인증 프로토콜을 제안하였는데, 이 또한 취약성이 존재하며 데이터베이스에서의 태그를 찾기 위해 전수조사를 해야 하기 때문에 효율성이 떨어지는 문제점이 있다. 본 논문에서는 Chien과 Chen이 제안한 기법을 분석하고 안전성과 효율성을 향상시킨 새로운 상호 인증 기법을 제안한다.

1. 서론

RFID(Radio Frequency IDentification) 시스템은 일정한 라디오 주파수 대역을 이용해 무선 방식으로 사물을 식별하는 시스템으로 기본적으로 태그(Tag)와 리더(Reader) 그리고 백-엔드-데이터베이스 (Back-End-Database)로 구성된다. 이러한 RFID 시스템은 태그와 리더의 무선 주파수를 이용한 통신으로 인해 물리적인 접촉 없이도 통신이 가능하여 인식률이 높고 인식 거리가 길며, 사물의 고유 식별 번호를 저장하고 있는 태그의 반복적인 재-쓰기(Re-Write)가 가능하다는 장점으로 인해 기존의 바코드 시스템을 대체하여 물류관리, 유통관리, 재고 관리 분야에서 널리 사용되고 있다. 2006년 ISO국제 표준화 회의에서 EPCglobal에서 제안한 Class-1 Generation-2(이하 Gen2)가 UHF-RFID 규격에 기초한 ISO 18000-6C로 편입됨으로써 표준화 문제도 해결되어 다양한 분야에서의 RFID 산업의 확산이 기대되어 진다[4].

하지만 RFID 시스템은 앞에서 언급한 여러 가지 장점을 가지고 있는 반면 무선 주파수를 이용한 통신으로 인해 정보노출, 위치추적, 위조 및 서비스 장애와 같은 보안 및 사용자 프라이버시 침해 문제를 발생한다. 지금까지 이를 보호하기 위한 많은 기법들이 제안되었다. 하지만 이들 기법은 안정성 측면에서 취약성이 존재하며 태그에서 암호학적 연산(대칭키 암호, 해쉬 함수 등)을 필요로 하기 때문에 저가 기반의 Gen2 태그에는 적합하지 않은 문제가 있다. 단지 몇몇 기법들만이 Gen2 기반의 RFID 시스템 환경에서 제안되었다[2,3,5]. 가장 최근에 Chien과 Chen[2]이 Karthikeyan et al[5]과 Duc et al[3]이 제안한 인증 기법들을 개선한 Gen2에서 지원하는 PRNG(Pseudo-Random Number Generator)와 CRC(Cyclic Redundancy Check)만을 사용한 Challenge-Response 기반의 상호 인증 기법을 제안하였다. 하지만 이 기법 역시 비동기화 문제가 발생하며 전방채널 안전성(Forward Security)을 만족하지 못하는 취약성이 존재한다. 또한 백-엔드-데이터베이스에서 특정 태그를 인증하기 위해 모든 태그에 대하여 전수조사(Exhaustive Search)를 해야 하는 비효율적인 문제가 존재한다. [6]에서는 이러한 전수조사 방식의 비효율성을 지적하고 블룸필터를 이용하여 전수조사를 하지 않고도 특정 태그를 찾는 멤버쉽 테스트 기법을 제안하였다.

이에 본 논문에서는 Chien과 Chen이 제안한 상호 인증 기법의 취약성을 지적하고 이를 개선한 Gen2 기반에서 안전성과 효율성을 향상시키는 새로운 상호 인증 기법을 제안한다. 백-엔드-데이터베이스에서의 효율성을 향상을 위해 [6]에서 제안한 기법을 Gen2기반에 적용하였다.

본 논문의 구성. 본 논문의 구성은 다음과 같다. 2장에서 제안 기법에 필요한 배경 지식을 알아보고 3장에서 본 논문에서 제안하는 상호 인증 프로토콜을 소개한다. 4장에서 제안하는 기법에 대한 안정성과 효율성을 언급 한 뒤 마지막으로 5장에서 결론을 맺는다.

2. 배경지식

+ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

2.1 블룸 필터(Bloom Filter)[1]

블룸필터(Bloom filter)는 주어진 원소가 사전에 정의되어진 집합 안에 포함되어 있는지 여부를 검사하는데 사용할 수 있는 자료 구조이다. 만약 블룸필터가 k개의 독립적인 해쉬 함수($h_1,h_2,.....h_k$)와 n개의 원소를 포함 하는 집합($S=\{s_1,s_2,.....s_n\}$)으로 만들어진 m 비트 스트링이라고 하자(블룸필터의 초기값은 0이다). 각각의 해쉬 함수는 0에서 m-1사이의 값을 갖고 이 값들은 블룸필터의 각각의 비트에 대응된다. m 비트의 블룸필터를 만들기 위해 각각의 원소 $s(\in S)$에 대해서 k개의 해쉬 함수($h_1,h_2,.....h_k$)값 $h_i(s)(1\le i\le k)$을 계산한 후 이 값에 해당하는 블룸필터의 비트를 1로 바꾼다. 만약 $h_i(s)=t$라고 하면 블룸필터의 t 번째 비트를 1로 바꾼다. 원소 $s'(\in S)$의 포함여부를 알아보려면 블룸필터의 $h_i(s')(1\le i\le k)$ 번째 비트가 모두 1인지 확인한다. 만약 k 비트 모두 1이면 s′가 원소이지만 k개 중 하나라도 0이라면 원소가 아니다.

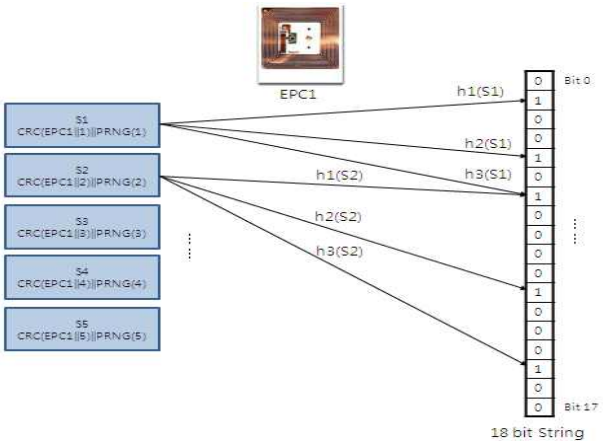

그림 1. 블룸필터 사용의 예

[그림 1]은 식별 정보 EPC_1의 값을 가지는 하나의 태그에 대하여 원소의 개수가 5, 서로 다른 함수의 개수 3, 블룸필터 스트링의 크기 m이 18일 때의 블룸필터를 만든 예이다. 태그에서 생성한 $CRC(EPC_1 \| j) \| PRNG(j)$ 값이 리더를 통하여 DB에 전송 되었을 때 DB는 $CRC(EPC_1 \| j) \| PRNG(j)$ 값에 k개의 해쉬 함수를 계산한 값이 m비트의 스트링에서 해당 위치에 모두 1로 되어있는지 체크함으로써 EPC_1에 대한 정보를 전수 조사를 하지 않고도 쉽게 해당 태그에 대한 데이터를 쉽게 찾을 수 있게 된다. 보다 자세한 사항은 3절에서 소개하도록 한다.

하지만 블룸 필터는 false positive error(집합에 포함되어 있지 않는 원소가 집합 안에 포함되어 있다고 잘못 판단하는 확률)가 존재한다. 다음 식은 false positive error가 일어날 확률을 말하며 사용하는 환경에 따라 k, n, m의 값을 조정하여 false positive error의 확률을 최적화 할 수 있다.

$$f=(1-(1-\frac{1}{m})^{kn})^{k}\approx(1-e^{-\frac{kn}{m}})^{k}$$

2.2 이전 기법들에 대한 분석

현재까지 RFID 시스템 보안 및 프라이버시 보호를 위한 많은 기법들이 연구되었다. 그러나 대부분의 기법들이 태그에서 해쉬 함수의 사용을 가정하기 때문에 암호학적 연산 능력이 없는 저가형 Gen2 태그에는 적합하지 않다. 또한 이들 기법은 보안 및 프라이버시 요구 사항을 완전히 만족시키지도 못하는 문제도 있다. 최근에는 [2,3,5]에서 Gen2 태그에 적합하면서 보안 및 프라이버시 문제를 해결하기 위한 기법들을 제안하였다. 하지만 Karthikeyan et al[5]과 Duc et al.[3]은 재생 공격 및 서비스 거부 공격에 취약성이 있으며 위치 추적도 가능한 문제점이 존재한다.

Chien과 Chen[2]는 이들 기법을 향상시킨 보다 강력한 Challenge-Response 기반의 상호 인증 기법을 제안하였다. 하지만 이 기법 역시 취약성이 존재하며 DB에서 효율성이 떨어지는 문제점이 있다. 다음은 Chien과 Chen 기법에 대한 안전성과 효율성을 분석한 것이다.

-안전성 분석

1) 서비스 거부 공격에 대한 취약성 : Chien과 Chen은 태그와 DB가 인증을 위해 사용하는 인증키 및 접근키의 동기화 유지를 위해서 DB에서 $(K_{old}, K_{new}),(P_{old}, P_{new})$ 쌍을 유지함으로써 서비스 거부 공격을 통한 비동기화 문제에 안전하다고 주장하고 있다. 하지만 공격자가 제안 기법은 리더에서 태그로 전송하는 M_2에 대하여 한 번의 서비스 거부 공격을 한다면 태그에서 키(K_i)가 업데이트 되지 않더라도 K_{old}에 K_i값이 저장되어 있기 때문에 동기화를 유지할 수 있다. 그러나 두 번 연속으로 서비스 거부 공격을 한다면 DB에 저장된 (K_{old}, K_{new})의 쌍과 태그에 저장된 K_i 사이에 더 이상 공통된 값이 없게 됨으로 동기화가 깨지게 된다. 이는 DB에서 매 세션마다 특정 태그를 인증할 때 K_i의 업데이트 상태를 체크하지 않아 발생하는 문제이다.

2) 전방 안정성에 대한 취약성 : Chien과 Chen은 공격자가 태그 메모리에 저장된 (K, P, EPC_x) 값을 알더라도 전방 안전성을 만족한다고 주장하고 있다. 하지만 공격자가 m번째 세션에서 메모리에 저장된 값 (K_m, P_m, EPC_x)을 알아낸다면 이전 n번째 세션에서 도청하여 저장하고 있는 (M_1, N_1, N_2) 값들과 함께 $M_1 \oplus CRC(EPC_x \| N_1 \| N_2)$을 계산하여 인증키 K_n을 알아 낼 수 있다. 따라서 공격자는 다음과 같이 $K_m = PRNG_{m-n}(K_n)$인지도 계산할 수 있게 되어 m번째 세션의 인증키와 n번째 세션의 인증키의 연계성을 찾을 수 있게 된다. 따라서 전방 채널 안전성을 만족하지 못하며 이로 인해 위치 추적도 가능하게 된다.

-DB에서의 효율성 분석

Challenge-Response 기반의 기법들은 상호 인증을 위해서 랜덤 값을 사용한다. 따라서 DB에서 인증하기위한 특정 태그를 찾기 위해서는 모든 태그에 대하여 전수조사를 해야 한다. [7]에서 이러한 전수조사 방식에 대한 비효율성을 테스트하였다. 그 결과 Gen2에 기반에서 2^{16} 태그가 존재할 때 백-엔드-데이터베이스에서 특정 태그를 찾는데 최악의 경우 7.87초가 걸리며 평균 4.10초가 걸리는 것을 확인할 수가 있다. 만약 100개의 태그를 한꺼번에 인식하기 위해서는 평균 410초가 소요되며, 이러한 인식 시간은 태그의 수가 증가할 때마다 비례하여 증가하게 된다. 따라서 이러한 전수조사는 매우 비효율적이다.

3. 제안하는 상호인증 프로토콜

3.1 용어 정의

[표1]은 제안 프로토콜에서 사용되는 용어를 정의한 것이다.

3.2 가정

이전에 제안되었던 기법들과 같이, 태그와 리더사이의 통신 채널은 무선 주파수를 이용한 안전하지 않은 채널이고, 백-엔드-데이터베이스와 리더의 통신 채널은 안전한 채널이라고 가정한다.

표기법	설 명
BF_x	각 Tag_x의 블룸필터 값
CRC	16비트 CRC 생성 함수
DB	백-엔드-데이터베이스
Data	각 Tag_x와 관련된 사물의 정보
EPC_x	각 Tag_x의 고유 ID
K_{old}	DB 와 Tag_x의 이전 인증키
K_{new}	DB 와 Tag_x의 새로운 인증키
K_i	i번째 세션의 인증키
PRNG	16비트 의사 난수 생성기
Reader	리더
Tag_x	태그

표 1. 용어 정의

3.3 제안 프로토콜

제안 상호 인증 프로토콜은 [그림 2]와 같으며 다음과 같이 초기 설정 단계와 상호 인증 단계로 나눌 수 있다.

3.3.1 초기 설정 단계

1) 각각의 Tag_x에 대하여 DB는 EPC_x, 초기 인증키 K_0을 생성하고 (EPC_x, K_0)를 Tag_x에 저장한다. 그리고 DB는 Tag_x에 대한 (1)EPC_x (2)이전의 인증키 $K_{old}(=K_0)$ (3)새로운 인증키 $K_{new}(=K_0)$ (4)BF(블룸 필터)의 값 (5)Tag_x에 대한 상품에 대한 정보 Data를 저장한다.

2) DB에서 특정 태그를 찾기 위해 블룸 필터(Bloom Filter)를 사용할 수 있다. 방법은 2장 블룸필터의 소개에서도 말했듯이 각각의 Tag_x의 EPC_x를 사용하여 원소의 집합을 만든다{$s_1,s_2,.....,s_n$}. 그리고 각각의 원소에 대하여 k개의 해쉬 함수의 값을 구하여 m비트의 블룸 필터 $BF(CRC(EPC_x \| 1) \| PRNG(1), CRC(EPC_x \| 2) \| PRNG(2),.....,CRC(EPC_x \| n) \| PRNG(n))$ 셋을 구성하고 이를 DB에 저장한다. 이후 리더로부터 전송된 T_1에 대한 멤버쉽 테스트를 통하여 원하는 태그의 데이터를 DB에서 쉽게 찾을 수 있으며 효율성을 높일 수 있다.

3.5.2 상호 인증 단계

1) (Challenge) Reader → Tag_x : R_r

리더는 랜덤 값 R_r을 생성하고 Tag_x에 R_r와 함께 질의 요청한다. R_r은 공격자의 스푸핑 공격 및 재생 공격을 막기 위해 사용된다.

2) (Response) Tag_x → Reader : T_1, T_2

Tag_x는 PRNG 함수를 사용하여 난수 j를 생성하고 $T_1=CRC(EPC_x \| j) \| PRNG(j)$를 계산한다. 그리고 T_1함께 리더로부터 전송된 랜덤 값 R_r, 인증키 K_i를 사용하여 $T_2=PRNG(R_r \| K_i \| T_1)$도 계산한 후 T_1, T_2를 리더에게 전송한다. T_1은 멤버쉽 테스트 시에 사용되며 T_2와 함께 매 세션 변경된다.

3) (Response) Reader → DB : R_r, T_1, T_2

리더는 Tag_x에서 전송된 T_1, T_2와 함께 자신이 생성한 R_r를 DB에 전송한다. 그리고 DB는 다음과 같은 과정을 수행한다.

(1) 멤버쉽 테스트를 행한다.($T_1 \in BF_i$)

-DB는 리더로부터 전송된 T_1에 대하여 간단한 연산과 비교과정을 통한 멤버쉽 테스트를 실행하고, Tag_x를 찾는다. 전수조사에 비해 특정 태그를 빠르고 쉽게 찾을 수 있다.

-찾지 못했다면 세션을 종료한다.

(2) Tag_x를 검증한다.($T_2=PRNG(R_r \| K_{old\ or\ new} \| T_1)$

-DB는 K_{old}의 값을 사용하여 인증하였는지 또는 K_{new}의 값을 사용하여 인증하였는지 체크한다. 그리고 K_d에 현재 인증 시 사용한 키(K_{old} or K_{new})를 임시 저장한다.

-인증하지 못했다면 세션을 종료한다.

(3) 리더와 Tag_x에게 전송할 (D_1,Data)을 생성한다.

-Tag_x에서 공유 인증키 K_i를 업데이트하기 할 때 정당한 DB를 검증하기 위한 $D_1=PRNG(EPC_x \| K_d \| T_1)$를 계산한다.

-DB는 D_1, 태그와 관련된 Data를 리더에게 전송한다.

(4) 인증키(K_{old}, K_{new})를 업데이트 한다.

-DB는 Tag_x를 인증시 K_{new}의 값으로 인증하였다면 다음과 같이 인증키를 업데이트 한다, $K_{old}=K_d$, $K_{new}=PRNG(K_d)$.

4) (Reply) DB → Reader : D_1, Data

정당한 리더는 Data를 읽고 사물의 정보를 얻는다, D_1은 Tag_x에 전송한다.

5) (Reply) Reader → Tag_x : D1

Tag_x는 $PRNG(EPC_x \| K_i \| T_1))$를 계산하여 리더로부터 전송 받은 D_1의 값과 비교 한다. 같다면 K_{i+1}의 값을 업데이트 하고 세션을 종료한다(상호 인증 완료), $K_{i+1}=PRNG(K_i)$. 다르다면 업데이트를 하지 않고 현재 세션을 종료한다.

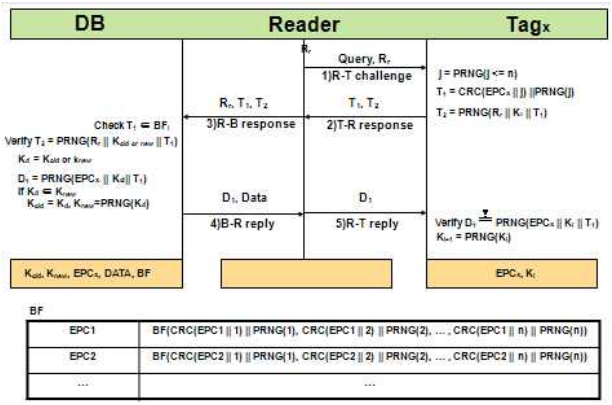

그림 2. 제안하는 상호 인증 프로토콜

4. 제안한 프로토콜 분석

4.1 안전성

-도청 공격

공격자가 태그에서 리더로 전송되는 정보(T_1, T_2)들을 도청한다고 할지라도 이는 공격자에게는 의미 없는 값이며 이로부터 태그와 관련된 정보를 알아 낼 수 없다. 따라서 안전하다.

-위치추적 공격

(a)구별 불가능성 : Tag_x는 리더가 질의(Query)를 할 때마다 랜덤 값 j를 사용하여 (T_1,T_2) 계산하기 때문에 매번 랜덤 값으로 응답한다. 따라서 리더는 수신한 데이터가 어떠한 태그에서 나온 값인지를 알 수 없어 구별 불가능성 만족한다.

(b)전방 안전성 : 물리적인 공격(Tampering Attack)을 통하여 태그의 메모리에 저장된 내용을 공격자가 알아낸다 할지라도 과거 도청한 (T_1,T_2)의 정보를 가지고 이전 인증키를 찾아 낼 수가 없

으며 이로부터 현재의 태그와의 연관성을 찾기도 힘들다. 따라서 전방 안전성을 만족한다.

따라서 두 가지 성질을 모두 만족함으로 익명성을 보장한다.

-스푸핑 공격

공격자는 자신이 생성한 랜덤 값 R_r와 함께 태그에 요청하여 (T_1, T_2)를 얻는다. 이 후 합리적인 리더가 자신이 생성한 랜덤 값 S' 함께 태그에 요청할 때 공격자는 자신이 저장하고 있던 값 (T_1, T_2)로 응답하여 스푸핑 공격을 시도 할 수 있다. 하지만 PRNG(S ‖ K_i ‖ T_1) ≠ PRNG(S' ‖ K_i ‖ T_1) 이기 때문에 공격자는 정당한 태그인척 할 수가 없다,

-재생 공격

공격자는 리더와 태그사이 전송되는 데이터를 도청하여 데이터를 저장하고 있다가 재전송 공격을 할 수 있다. 하지만 이와 같은 경우에도 스푸핑 공격에서와 마찬가지로 DB에서의 인증과정을 통과 할 없으며 탐지가 가능하기 때문에 안전하다.

-서비스 거부 공격

공격자는 상호 인증 5)단계에서 강한 전파의 사용 및 가로채기 공격을 통하여 D_1이 전송되는 것을 막음으로써 태그에서의 인증키 K_i의 K_{i+1}로의 업데이트를 방해할 수 있다. 하지만 이와 같은 경우가 발생하더라도 이후 세션에서 DB는 이전 공유키 K_{old}를 사용하여 인증하기 때문에 동기화를 유지할 수 있다.

[표 2]은 Gen2 기반에서 제안된 기법들에 대하여 안전성을 비교하였다. 표에서 보듯이 본 논문에서 제안하는 기법은 기본의 Gen2에 기반에서 제안된 기법들과 다르게 보안 및 프라이버시 보호를 위한 요구 사항을 모두 만족함을 볼 수 가 있다.

제안 기법	[5]	[3]	Our Scheme
프라이버시	O	O	O
익명성	X	X	O
스푸핑 공격 저항	X	O	O
재생 공격 저항	X	O	O
DOS 공격 저항	X	X	O
전방 안전성	X	X	O
상호 인증	O	O	O

표 2. Gen2 기반 제안 기법들의 안전성 비교

4.2 효율성

-태그에 대한 효율성

제안 기법은 단지 Gen2에서 지원하는 CRC 함수와 PRNG 함수만을 사용하여 기존의 기법들이 만족하지 못하는 보안 및 프라이버시 문제를 해결하였다. 또한 태그에서 EPC와 DB와의 공유하는 인증키 K값만을 저장함으로 해서 가격이 비싼 비휘발성 메모리의 사용을 최소화하였다.

-DB에 대한 효율성

본 논문에서 제안하는 기법의 효율성을 Chien과 Chen의 기법과 비교하기 위해 태그의 개수를 최대 2^{16}개라고 가정한다. Chien과 Chen의 기법에서 태그가 보내는 M_1값의 길이가 CRC의 출력값의 길이와 같기 때문에 만약 태그의 수가 2^{16}개보다 많다면 DB는 태그를 유일하게 결정할 수 없게 된다. 본 기법은 블룸필터 기법을 사용함으로써 백-엔드-데이터베이스에서 특정 태그를 찾기 때 전수조사를 하지 않아도 된다. 따라서 태그를 인증하는데 걸리는 시간이 태그의 수에 상관이 없이 일정함으로 효율적이다.

[표 3]은 Gen2 기반에서 제안된 기법들에 대한 효율성을 분석하였다. 표에서도 보듯이 제안 기법은 태그에서의 비휘발성 메모리의 사용을 하나 줄임으로써 저장량을 최소화 하였다. 또한 기존 기법들과 달리 DB에서 전수 조사 방식을 사용하지 않음에 따라 계산량을 최소화하여 효율성을 높였다. 그리고 상호 인증에서 동기화를 유지하기 위해 필요한 최소한의 통신량을 유지함으로써 통신량에서의 유연함을 보였다.

프로토콜			[5]	[3]	Our Scheme
저장량	태그		3l	3l	2l
	DB		3l	5l	4l+|BF|
계산량	태그	CRC	3	2	1
		PRNG	2	3	5
	DB	Search	H	H	L
통신량			8	5	5

l : 하나의 데이터 유닛에 대한 비트의 길이

H : High, L : Low

표 3. Gen2 기반 제안 기법들의 효율성 비교

5. 결론

본 논문에서는 최근 Chien과 Chen이 제안한 Gen2 기반의 상호 인증 기법에 대하여 취약성을 분석하고 보다 안전한 새로운 상호 인증 기법을 제안하였다. 본 기법은 안전성을 모두 만족함과 동시에 DB에서 태그 인증 시 효율성을 향상 시킨 RFID 시스템에 적합한 상호 인증 프로토콜을 제안하였다.

참고 문헌

[1] Andrei broder and Michael Mitzenmacher, "Network Applications of Bloom Filters : A Survey", Internet Mathematics, vol 1, no 4, 2004, pp 485-509(SAC), 2005.

[2] H.Y. Chien and Che-Hao Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards", In Computer Standards & Interfaces, 2006

[3] D.N. Duc, J. Park, H. Lee, K. Kim, "Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning", The 2006 Symposiumon Cryptography and Information Security, 2006.

[4] EPCglobal Inc., "Radio Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960MHz Version 1.0.9.,http://www.EPCgloballinc.org

[5] S. Karthikeyan, M. Nesterenko, "RFID security without extensive cryptography", Proceedings of the 3rd ACM Workshop on Security of AdHoc and Sensor Networks, 2005, pp. 63 - 67.

[6] 김진호, 서재우, 이필중, "멤버쉽 테스트를 이용한 RFID 인증 프로토콜", 2007년도 정보보호학회 하계학술대회, vol. 17, no. 1, 2007, pp. 93-98

[7] 원태연, 천지영, 최은영, 이동훈, "RFID 보안시스템에서 전수조사 방식에 대한 성능테스트", 2007년도 정보보호학회 동계학술대회, vol. 17, no. 2, 2007, pp. 203-206